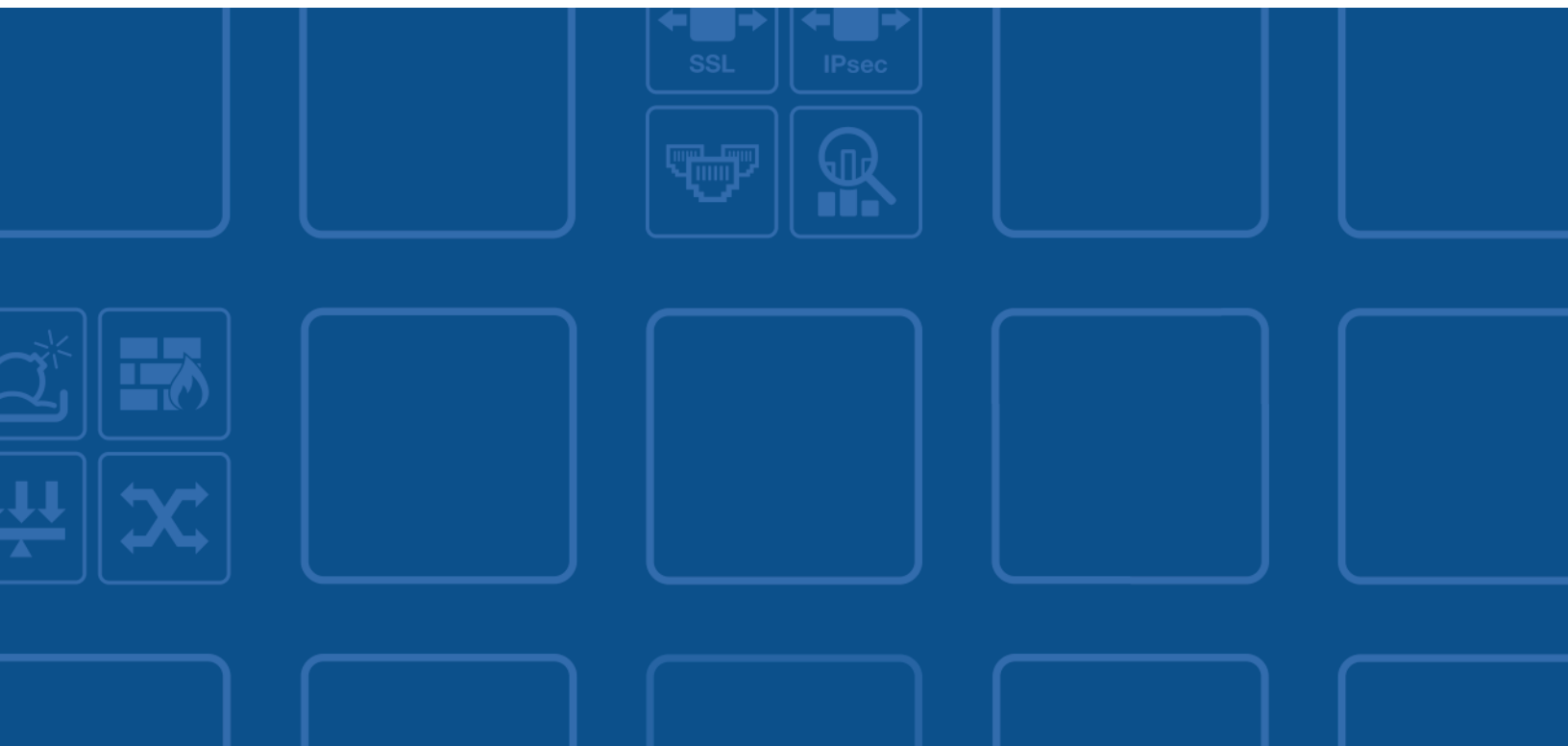
FORTINET
High Performance Network Security

FortiAnalyzer - Release Notes

VERSION 5.4.0



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

December 29, 2016

FortiAnalyzer - Release Notes

05-540-301358-20161229

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-02-17	Initial Release.
2016-02-18	Corrected FortiGate supported model and FortiClient supported version
2016-02-19	Updated FortiAnalyzer 5.4.0 support information.
2016-02-23	Removed Hebrew, Hungarian, and Russian from language support
2016-04-26	Added 307847 to Resolved Issues
2016-05-25	Added FAZ-400E for version 5.4 to Supported Models
2016-06-22	Added FAZ-1000E for version 5.4 to Supported Models
2016-10-28	Added link to the FortiAnalyzer Upgrade Guide to Special Notices > Generate reports during the database rebuild.
2016-12-28	Updated What's New to clarify that the new WiFi summary views only support logs from FortiOS 5.4.x.
2016-12-29	Added special notice about Hyper-V FortiAnalyzer-VM running on an AMD CPU.

Introduction

This document provides the following information for FortiAnalyzer version 5.4.0 build 1019:

For more information on upgrading your FortiAnalyzer device, see the *FortiAnalyzer Upgrade Guide*.

Supported models

FortiAnalyzer version 5.4.0 supports the following models:

FortiAnalyzer	FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, and FAZ-4000B.
FortiAnalyzer VM	FAZ-VM32, FAZ-VM64, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.

What's new in FortiAnalyzer version 5.4.0

The following is a list of new features and enhancements in FortiAnalyzer version 5.4.0.

- New GUI look
- Remote SQL database deprecated
- Device support improvements
- Log forwarding improvements
- Log storage improvements
- Fetch offline logs
- FortiClient improvements
- FortiView improvements, including the following new summary views:
  - FortiView > Summary
  - FortiView > Summary > Threats: Threat Map
  - FortiView > Summary > Traffic: Policy Hit
  - FortiView > Summary > Application & Websites: Top Browsing Users

  - FortiView > Summary > WiFi: Authorized APs, Authorized SSIDs, WiFi Clients
  - FortiView > Summary > System: Storage Statistics
  - Failed Authentication Attempt
  - FortiView > Summary > Endponts: All FortiClient endpoints registered to FortiGates
- Reports improvements
- Others
  - Improved Event Management usability
  - Added Factory Reset option to Event Handler
  - Improved Action and Security Action for the Traffic Log
  - Improved HA Conversion efficiency
  - Correlated FortiClient Logs with FortiOS Logs for Application Detection
  - Added logging support for FortiDDoS
  - JSON API Syntax Validation for Report Configuration
  - Added SSN/Credit DLP Charts
  - PCI DSS Compliance Report
  - Added View Related Logs Option in FortiView
  - Added the ability to clone a chart from report layout
  - Added options for chart import and export
  - Added CVE Information to FortiView and Reports
  - Supporting EMS Managed Endpoint Logs
  - Support FortiOS Web Application Firewall (WAF) and GTP Logs

The following summary views only support logs from FortiOS 5.4.x: *FortiView > Summary > WiFi: Authorized APs, Authorized SSIDs, WiFi Clients*.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 5.4.0.

Hyper-V FortiAnalyzer-VM running on an AMD CPU

A Hyper-V FAZ-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

SQL Storage Settings for Collector Mode

During upgrade to FortiAnalyzer 5.4.0, the SQL database in units running in Collector mode are disabled to optimize performance. You can re-enable the SQL storage settings to view logs and analytics with the following CLI command:

```
config system sql
set status local
end
```

Authentication Settings for Log Aggregation

FortiAnalyzer version 5.4.0 requires an administrator to be defined on the log aggregation server. For authentication to the log aggregation server, the administrator and its password must be set on all log aggregation forwarders.

Log Aggregation or Forwarding

FortiAnalyzer 5.4 cannot aggregate or forward logs to FortiAnalyzer 5.2 units. Please use the same FortiAnalyzer 5.4 version across all units.

SSLv3 on FortiAnalyzer-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiAnalyzer-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
    set ssl-protocol t1sv1
end
```

SQL database rebuild

FortiAnalyzer can receive new logs during SQL database rebuild.

FortiView, Log View, Event Management, and Reports are also available.However, all scheduled reports are skipped. It is recommended to generate reports only after finishing the database rebuilding process.

Report grouping

If you are running a large number of reports which are very similar, you can significantly improve report generation time by grouping the reports. Report grouping can reduce the number of hcache tables and improve auto-hcache completion time and report completion time.

Step 1: Configure report grouping

To group reports whose titles contain the string `Security_Report` and are grouped by device ID and VDOM, enter the following CLI commands:

```
config system report group
   edit 0
      set adom root
      config group-by
         edit devid
         next
         edit vd
         next
   end
   set report-like Security_Report
   next
end
```

Notes:

1. The `report-like` field is the name pattern of the report that will utilize the `report-group` feature. This string is case-sensitive.
2. The `group-by` value controls how cache tables are grouped.
3. To see a listing of reports and which ones have been included in the grouping, enter the following CLI command:

   ```
   execute sql-report list-schedule <ADOM>
   ```

Step 2: Initiate a rebuild of hcache tables

To initiate a rebuild of hcache tables, enter the following CLI command:

```
diagnose sql rebuild-report-hcache <start-time> <end-time>
```

Where `<start-time>` and `<end-time>` are in the format: `<yyyy-mm-dd hh:mm:ss>`.

Step 3: Perform an hcache-check for a given report

Perform an hcache-check for a given report to ensure that the hcache tables exactly match the start and end time frame for the report time period. Enter the following CLI command:

```
execute sql-report hcache-check <adom> <report_id> <start-time> <end-time>
```

If you do not run this command, the first report in the report group will take a little longer to run. All subsequent reports in that group will run optimally.

Generate reports during the database rebuild

After FortiAnalyzer is upgraded, the system may need to rebuild databases due to schema changes. Please note that the ability to generate accurate reports will be affected until the rebuild is complete.

For a list of the FortiAnalyzer upgrade paths that require database rebuilds, see the FortiAnalyzer 5.4.0 Upgrade Guide.

Special characters in report name

FortiAnalyzer version 5.2 does not support the following special characters in report's name:

```
\ / ' " > < & , | # ? % $ +
```

If you wish to import a report, please make sure the above special characters are not used. Otherwise, FortiAnalyzer may not display the name properly.

Required changes to dataset

The following rules must be followed by any existing or new datasets:

If your dataset references any IP related data, such as `srcip` or `dstip`, please use the `ipstr('…')` function to convert an IP address for proper display. For example, `ipstr('srcip')` returns the source IP in a string.

The column, `status`, has been changed to `action`. Please replace `status` with `action` in dataset query for proper status.

FortiAnalyzer VM

In VM environments, upgrade your VM server to latest stable update and patch release offered by the VM host server provider before installing or upgrading FortiAnalyzer VM.

FortiAnalyzer VM license check

As a part of the license validation process, FortiAnalyzer VM compares its IP addresses with the IP information in the license file. If the IP addresses do not match, FortiAnalyzer VM returns the error `IP does not match` as part of the CLI command `get system status` output. If a new license has been imported or the IP address of FortiAnalyzer VM has been changed, the FortiAnalyzer VM will reboot itself for the system to validate the change and operate with a valid license.

Extended UTM log for Application Control

For FortiOS 5.0 devices, the application control log is not visible until you enable the extended UTM log in the FortiOS CLI.

To enable extended UTM log, use the following CLI command:

```
config application list
   edit <name>
      set extended-utm-log enable
end
```

Distributed upgrades

For Collector/Analyzer architecture upgrades, Fortinet recommends upgrading the Analyzer first.

Upgrading the Collector first could impact the Analyzer's performance.

Manually Starting LVM Service

If FortiAnalyzer does not have a valid logical volume management (LVM) configuration, LVM service will not start upon boot-up when the disk already contains data. Users will need to run `execute lvm start` to enable the service.

Upgrade Information

Upgrading to FortiAnalyzer 5.4.0

For information about upgrading your FortiAnalyzer to version 5.4.0, see *FortiAnalyzer 5.4.0 Upgrade Guide*.

Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. To verify the integrity of the download, select the *Checksum* link next to the *HTTPS* download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for Amazon AWS, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bits Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bits firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.OpenXen.zip`: Download the 64-bits package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bits package for a new FortiAnalyzer VM installation. This package contains the Citrix XenServer Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bits firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.kvm.zip`: Download the 64-bits package for a new FortiAnalyzer VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Hyper-V Server

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

VMware ESX/ESXi

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager product data sheet available on the Fortinet web site, http://www.fortinet.com/products/fortimanager/virtualappliances.html. VM installation guides are available in the Fortinet Document Library.

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 file folder.

Product Integration and Support

FortiAnalyzer 5.4.0 support

The following table lists FortiAnalyzer version 5.4.0 product integration and support information:

Web Browsers	• Microsoft Internet Explorer 11.0 • Mozilla Firefox version 42 • Google Chrome version 47 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 5.4.0 • 5.2.0 to 5.2.6 • 5.0.4 to 5.0.12 • 4.3.2 to 4.3.18
FortiAnalyzer	• 5.4.0 • 5.2.0 to 5.2.5 • 5.0.0 to 5.0.11
FortiCache	• 3.1.1 • 3.0.0 to 3.0.4
FortiClient	• 5.4.0 • 5.2.0 and later
FortiMail	• 5.3.1 • 5.2.6 • 5.1.5 • 5.0.8
FortiManager	• 5.4.0 • 5.2.0 and later • 5.0.0 and later
FortiSandbox	• 2.1.2 • 1.4.0 and later • 1.3.0 • 1.2.0 and 1.2.3

FortiSwitch ATCA	• 5.2.3 • 5.0.0 and later • 4.3.0 and later • 4.2.0 and later
FortiWeb	• 5.5.1 • 5.4.0 • 5.3.7 • 5.2.4 • 5.1.4 • 5.0.6
FortiDDoS	• 4.1.11
Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS • Citrix XenServer 6.2 • Linux KVM Redhat 6.5 • Microsoft Hyper-V Server 2008 R2, 2012 & 2012 R2 • OpenSource XenServer 4.2.5 **VMware** • ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0

Always review the Release Notes of the supported platform firmware version before upgrading your device.

Feature support

The following table lists FortiAnalyzer feature support for log devices.

Feature support per platform

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer	✓		✓	
FortiCache	✓		✓	✓

Platform	Log View	FortiView	Event Management	Reports
FortiClient registered to FortiGate	✓	✓		✓
FortiClient registered to FortiClient EMS	✓			✓
FortiDDoS	✓	✓	✓	✓
FortiMail	✓		✓	✓
FortiManager	✓		✓	
FortiSandbox	✓		✓	✓
FortiWeb	✓		✓	✓
Syslog	✓		✓	

Language support

The following table lists FortiAnalyzer language support information.

Language support

Language	GUI	Reports	Documentation
English	✔	✔	✔
Chinese (Simplified)	✔	✔	
Chinese (Traditional)	✔	✔	
French		✔	
Japanese	✔	✔	
Korean	✔	✔	
Portuguese		✔	
Spanish		✔	

To change the FortiAnalyzer language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can import language translation files for these languages via the command line interface using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <sftp <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information, see the *FortiAnalyzer CLI Reference*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiAnalyzer, FortiMail, FortiManager, FortiWeb, FortiCache, and FortiSandbox models and firmware versions can log to a FortiAnalyzer appliance running version 5.4.0. Please ensure that the log devices are supported before completing the upgrade.

FortiGate models

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-50E, FG-51E, FG-60D, FG-60D-POE, FG-70D, FG-70D-POE, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-140D, FG-140D-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FGT-280D-POE, FGT-300D, FG-400D, FG-500D, FG-600C, FG-600D, FG-800C,FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D **FortiGate 5000 Series:** FG-5001C, FG-5001D **FortiGate DC:** FG-600C-DC, FG-800C-DC, FG-1000C-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810D-DC **FortiGate Low Encryption:** FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **FortiWiFi:** FWF-30D, FWF-30E, FWF-50E, FWF-51E, FWF-30D-POE, FWF-60D, FWF-60D-POE, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiGate Rugged:** FGR-90D	5.4

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600D, FG-900D, FG-600C, FG-620B, FG-621B, FG-800C, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C,FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, G-3700D-DC, FG-3810A-DC, FG-3810D-DC, FFG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-310B-LENC, FG-600C-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-100C **FortiGate VM:** FG-VM-Azure, FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B, FCT-5902D	5.2

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-700D, FG-800C, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:**FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-60D-3G4G-VZW, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-90D, FGR-100C **FortiGateVoice:** FGV-40D2, FGV-70D4 **FortiGate VM**: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B	5.0

FortiCarrier Models

Model	Firmware Version
FortiCarrier: FCR-3240C, FCR-3600C,FCR-5001C **FortiCarrier DC:** FCR-3240C-DC, FCR-3600C-DC **FortiCarrier VM:** FCR-VM, FCR-VM64	5.4
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C,FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D **FortiCarrier DC:** FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-Vm64-XEN	5.2
FortiCarrier: FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C **FortiCarrier DC:** FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64	5.0

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E,FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2

Model	Firmware Version
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiMail models

Model	Firmware Version
FortiMail: FE-200D, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.2
FortiMail: FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.1.4
FortiMail: FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.0.7

FortiManager models

Model	Firmware Version
FortiManager: FMG-200D, FMG-300D, FMG-300E, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, and FMG-4000E. **FortiManager VM:** FMG-VM32, FMG-VM64, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMG-VM64-KVM, FMG64-AWS, and FMG-VM64-HV.	5.4
FortiManager: FMG-100C, FMG-200D, FMG-300D, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E **FortiManager VM:** FMG-VM32, FMG-VM64,FMG-VM64-AWS, FMG-VM64-HV, FMG-VM64-KVM, FMG-VM64-XEN	5.2
FortiManager: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, and FMG-5001A. **FortiManager VM:** FMG-VM32, FMG-VM64, FMG-VM64-HV	5.0

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-3500D	2.1.0
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0.0 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ACTA models

Model	Firmware Version
FortiController: FTCL-5902D	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

FortiWeb models

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, and FWB-HYPERV	5.3.7
FortiWeb: FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D **FortiWeb VM:** FWB-VM64	5.3.3
FortiWeb: FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D **FortiWeb VM:** FWB-VM64, FWB-HYPERV,FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER	5.2.4

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D **FortiCache VM:** FCH-VM64	3.0.0 and later

Resolved Issues

The following issues have been fixed in FortiAnalyzer version 5.4.0. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
298415	FortiAnalyzer cannot add FortiController 5103B as a syslog device.
292606	FortiAnalyzer cannot accept logs from FortiADC.
279319	Non-existing VDOMs with strange characters are displayed.

Event Management

Bug ID	Description
299664	The RPI field is missing from Syslog alert.
287216	Event Handlers returns SQL error: duplicated key (Alert ID) when inserting alert_logs.
284440	There is an invalid *Ref Field* in the FortiGate Logs.
270264	Change Device ID to Device Name in an Email subject line subject line.

FortiView

Bug ID	Description
298726	Top Threats may not show any results that reflect the corresponding threat logs.
291597	The Application icons are not displayed in FortiView and Log View.
280309	FortiView Resource Usage does not display peak values.
280181	FortiAnalyzer does not display IP/MAC information in DHCP logs.

Logging

Bug ID	Description
307732	F3K2D-DC logs are recognized as Syslogs.

Bug ID	Description
299509	IPv6 logs that are sent to Syslog server via log forwarding are different from IPv6 logs that are sent directly from FortiGate.
291652	Fortilogd may be blocked by slow TCP log forwarding and stop receiving incoming logs.
286804	Search takes longer than expected and may return unexpected results.
286190	The “Last 5 min” interval option is missing from the FortiLog Time Interval List .
284658	FortiAnalyzer does not refresh the list of logs with the *Go* button.
281953	Advanced ADOM mixes up logs from different VDOMs.
280891	Several fields are missing when viewing FortiSandbox logs.
280873	String value in the Extension Field that is formatted using CEF is surrounded by quotes.
280578	When the Language setting is set to Japanese, FortiAnalyzer shows columns with the same heading.
280192	Base64 encoded "log-attack-context" log is not readable.
280192	Base64 encoded `log-attack-context` events are not readable on FortiAnalyzer.
280053	Attack Context ID for Intrusion Prevention logs are not parsed properly.
278804	FortiAnalyzer does not restrict the number for Last N days in Log View.
278453	FortiAnalyzer returns an error and stops a query when the Source IP is an invalid IP address.
278077	Traffic log table still displays the Date/Time column even though it has been disabled via Column Settings.
276989	Scan Start and End times should be displayed in a readable format instead of in epoch mode.
276491	GTP specific fields are missing in Event Log Viewer after an upgrade.

Reporting

Bug ID	Description
300877	Users are unable to choose columns when creating a table chart from dataset.
300569	When there are many hcache tables, the SQL query for report generation may fail.
298217	The report generated for "Active Traffic Users" has data inconsistent with the dataset output.

Bug ID	Description
295987	The “Top 20 Bandwidth Users” report that runs with the “Webfilter-Top-Web-Users-By-Bandwidth” data set may not return correct data.
292983	The apprisk-ctrl-Common-Virus-Botnet-Spyware dataset may filter out botnet applications.
291808	Some VDOMs are missing under the Configuration tab of a report.
286653	When selecting a background image, the footer background color does not apply to the cover page.
286588	Creating `hcache` does not work after enabling the *Report Group*.
284133	When using the `$flex_timescale`, the Start time and End time are not correct in the SQL.
283433	User filter does not work when the username contains the `\` character.
275394	FortiAnalyzer loses auto column update in chart when the dataset is changed.
272777	When query results contain the `#` character, it cannot be displayed in the table chart.
262593	Japanese characters in a PDF formatted report are displayed in an unexpected front style.
257691	Report line chart limits the number of items depending on the period specified for the report.
231536	A Group Report should not be generated when the Multiple Reports (Per-Device) option is selected.

System Settings

Bug ID	Description
278334	FortiAnalyzer displays inconsistent behavior for read-only admin profiles.
270785	When the license count is exceeded, the alert message does not appear.

Others

Bug ID	Description
307847	Removed the maintainer account from FortiAnalyzer.
306160	Syslog is trimmed when being forwarded to a syslog server.
296481	The getFazGeneratedReport XML call should include macro data in the report_data.txt file.

Bug ID	Description
296228	FortiAnalyzer should support TLS v1.1 and v1.2.
295051	Within a XML response, the report name always has prefix "S-{layout-id}_t{layout-id}-".
294453	Some SOAP API calls may not close connections.
291013	Oftpd may crash in some situations.
286512	Device version is not set in the CEF message header field.
286498	FortiAnalyzer does not back up logs to FTP when using log-file-archive-name extended .
283832	`Oftp` keeps updating the address from multiple VDOMs when the FortiAnalyzer override is enabled in each of the VDOMs.
279760	FortiAnalyzer returns an error when running `searchFazLog` using *duration* or *sentbyte* as `searchCriteria` with the XML API.
277478	Several *ERROR: extra data after last expected column* messages appear in the `pgsvr.log`.
275008	The `fazmaild daemon` stops working.
241924	The Drilldown to UTM tabs of FortiGate do not show the correct UTM log entry when the device is FortiAnalyzer.

Known Issues

The following issues have been identified in FortiAnalyzer version 5.4.0. For inquires about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Reporting

Bug ID	Description
295199	Percentage on Storage Statistics can be over 100%.

System Settings

Bug ID	Description
299318	The Actual day for Archive should not be longer than the Config day.

FORTINET®

High Performance Network Security